What is claimed is:

[Claim 1] 1. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises transactional account information, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and

(iii) wherein the electronic communication is communicated electronically from the sender; and

(c) validating the identity of the sender for the electronic communication by only performing the steps of,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public

key and the digital signature comprises decrypting the digital signature using the public key,

whereby a comparison resulting in a match validates the identity of the sender.

[Claim 2] 2. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises transactional account information, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and

(iii) wherein the electronic communication is communicated electronically from the sender; and

(c) validating the identity of the sender for the electronic communication by only performing the steps of,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key,

whereby a comparison resulting in a match validates the identity of the sender, and wherein neither a PIN nor a password is required to be transmitted to the receiver for validating the identity of the sender.

[Claim 3] 3. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises transactional account information and the sender identity information comprises other than an account number, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and

(iii) wherein the electronic communication is communicated electronically from the sender; and

(c) validating the identity of the sender for the electronic communication by,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key,

whereby a comparison resulting in a match validates the identity of the sender.

[Claim 4] 4. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a) initially, associating by the receiver sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises transactional account information, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and

(iii) wherein the electronic communication is communicated electronically from the sender, and

(iv) wherein the electronic communication is the only electronic communication received from the sender by the receiver relating to the action; and

(c) validating the identity of the sender for the electronic communication by,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key,

whereby a comparison resulting in a match validates the identity of the sender.

[Claim 5] 5. The method of claims 1, 2, 3, or 4, wherein the electronic communication includes the electronic message.

[Claim 6] 6. The method of claims 1, 2, 3, or 4, wherein the electronic message is implied from the receipt of the electronic communication.

[Claim 7] 7. The method of claims 1, 2, 3, or 4, wherein the digital signature is derived within a smart card of the sender.

[Claim 8] 8. The method of claims 1, 2, 3, or 4, wherein the digital signature is received from the sender within a terminal of a third-party and then forwarded to the receiver.

[Claim 9] 9. The method of claims 1, 2, 3, or 4, wherein the electronic communication is received over a secure network.

[Claim 10] 10. The method of claims 1, 2, 3, or 4, wherein the electronic communication is received over an insecure network.

[Claim 11] 11. The method of claim 10, wherein the network comprises the Internet.

[Claim 12] 12. The method of claims 1, 2, 3, or 4, wherein the electronic communication is received encrypted.

[Claim 13] 13. The method of claims 1, 2, 3, or 4, wherein the electronic communication is received unencrypted.

[Claim 14] 14. The method of claims 1, 2, 3, or 4, wherein the receiver is a financial institution and the action on the account comprises a financial transaction.

[Claim 15] 15. The method of claims 1, 2, 3, or 4, wherein the electronic communication includes the public key.

[Claim 16] 16. The method of claims 1, 2, or 4, wherein the sender identity information comprises the account number.

[Claim 17] 17. The method of claims 1, 2, or 4, wherein the sender identity information comprises other than the account number.

[Claim 18] 18. The method of claims 1, 2, 3, or 4, wherein the public key was associated with the account when the account was first established.

[Claim 19] 19. The method of claim 18, wherein the public key was provided by the sender to the receiver.

[Claim 20] 20. The method of claim 18, wherein the public key was provided to the sender by the receiver.

[Claim 21] 21. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes information required to process the action.

[Claim 22] 22. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes a personal identification number (PIN).

[Claim 23] 23. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes an account balance representing funds in the account.

[Claim 24] 24. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes information validated when the account was established.

[Claim 25] 25. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes information that was validated in a face-to-face acknowledgement between the sender and the receiver.

[Claim 26] 26. The method of claims 1, 2, 3, or 4, wherein the account comprises a checking account.

[Claim 27] 27. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes a history of ledger transactions in the account.

[Claim 28] [c28] 28. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes the social security number of the sender.

[Claim 29] 29. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes the address of the sender.

[Claim 30] 30. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes the mother's maiden name of the sender.

[Claim 31] 31. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes entity information of the sender.

[Claim 32] 32. The method of claims 1, 2, 3, or 4, wherein the transactional account information only includes entity information of the sender.

[Claim 33] 33. The method of claims 1, 2, 3, or 4, wherein the transactional account information includes business process information.

[Claim 34] 34. The method of claims 1, 2, 3, or 4, wherein the transactional account information is stored in fields in records in a computer database.

[Claim 35] 35. The method of claim 34, wherein the records comprise an account file.

[Claim 36] 36. The method of claim 35, wherein the records further comprise a transactions file.

[Claim 37] 37. The method of claims 1, 2, 3, or 4, wherein the digital signature is derived within a hand-held device of the sender.

[Claim 38] 38. The method of claims 1, 2, 3, or 4, wherein the function of the electronic message comprises applying a hashing algorithm to the electronic message.